

WHAT IS CLAIMED IS:

1. A key management device for provision of a security
service in an Ethernet-based passive optical network,
5 comprising:

an optical line terminal for sending a discovery gate
message to discover an optical network unit for data
transmission, and, if said optical network unit receives said
discovery gate message and then requests data communication,
10 sending an encrypted registration message including a permanent
medium access control (MAC) address of said optical network
unit to said optical network unit to notify said optical
network unit that it has been registered and an encrypted
general gate message including said permanent MAC address of
15 said optical network unit to said optical network unit to
allocate a time slot to said optical network unit; and

said optical network unit for receiving said discovery
gate message and then sending an encrypted registration request
message to said optical line terminal to request the data
20 communication therewith and an encrypted registration
acknowledgement message to said optical line terminal to
respond to said registration message.

2. The key management device as set forth in claim 1,
25 wherein said discovery gate message is periodically sent.

3. The key management device as set forth in claim 1,
wherein said discovery gate message includes a time slot field
allocated to said optical network unit for registration
thereof, a capability of said optical line terminal, a public
5 key of said optical line terminal, and a nonce encrypted by a
private key of said optical line terminal for signature.

4. The key management device as set forth in claim 1,
wherein said registration request message includes a physical
10 ID capability, a capability of said optical network unit, an
echo of a capability of said optical line terminal, a session
key, a nonce decrypted by a public key of said optical line
terminal, and a nonce created for signature of said optical
network unit.

15

5. The key management device as set forth in claim 4,
wherein said physical ID capability, said capability of said
optical network unit, said echo of said capability of said
optical line terminal, said nonce decrypted by said public key
20 of said optical line terminal and said nonce created for the
signature of said optical network unit are encrypted using said
session key.

6. The key management device as set forth in claim 4,
25 wherein said session key is encrypted using said public key of

said optical line terminal.

7. The key management device as set forth in claim 1,
wherein said registration message further includes a physical
5 ID list, an echo of a capability of said optical network unit,
and a signature of said optical network unit.

8. The key management device as set forth in claim 1,
wherein said general gate message further includes a time slot
10 field for upstream transmission of said optical network unit.

9. The key management device as set forth in claim 8,
wherein said general gate message is encrypted using a session
key.
15

10. The key management device as set forth in claim 1,
wherein said registration acknowledgement message includes a
session key encrypted by a public key of said optical line
terminal, and an echo of a registered physical ID.
20

11. The key management device as set forth in claim 10,
wherein said registration acknowledgement message is encrypted
using said session key.

25 12. The key management device as set forth in claim 1,

wherein said optical line terminal includes:

a public key processor for creating a public key to be included in said discovery gate message, and encrypting and decrypting said public key;

5 a session key processor for decrypting said registration request message and registration acknowledgement message from said optical network unit using a session key, and encrypting said general gate message and registration message using said session key;

10 a private key processor for creating a private key using said public key for encryption of messages to be transmitted to said optical network unit and decryption of messages received from said optical network unit, and encrypting and decrypting said private key; and

15 storage means for storing and managing said public key, session key and private key.

13. The key management device as set forth in claim 1, wherein said optical network unit includes:

20 a session key processor for creating a session key for encrypted communication with said optical line terminal, encrypting a part of said registration request message using said session key, decrypting said registration message and general gate message from said optical line terminal using
25 said session key and encrypting said registration

acknowledgement message using said session key;

a public key processor for encrypting said session key
using a public key from said optical line terminal; and

storage means for storing said session key and public
5 key.

14. A method for session key distribution between an
optical line terminal and an optical network unit in a key
management method for provision of a security service in an
10 Ethernet-based passive optical network, comprising the steps
of:

a), by said optical line terminal, sending a discovery
gate message to discover said optical network unit for data
transmission;

15 b), by said optical network unit, receiving said
discovery gate message and then sending an encrypted
registration request message to said optical line terminal to
perform data communication therewith;

c), by said optical line terminal, sending an encrypted
20 registration message including a permanent MAC address of said
optical network unit to said optical network unit to notify
said optical network unit that it has been registered;

d), by said optical line terminal, sending an encrypted
general gate message including said permanent MAC address of
25 said optical network unit to said optical network unit to

allocate a time slot to said optical network unit; and

e), by said optical network unit, sending an encrypted registration acknowledgement message to said optical line terminal to respond to said registration message.

5

15. The session key distribution method as set forth in claim 14, wherein said discovery gate message is periodically sent.

10

16. The session key distribution method as set forth in claim 14, wherein said discovery gate message includes a time slot field allocated to said optical network unit for registration thereof, a capability of said optical line terminal, a public key of said optical line terminal, and a
15 nonce encrypted by a private key of said optical line terminal for signature.

20

17. The session key distribution method as set forth in claim 14, wherein said registration request message includes a
physical ID capability, a capability of said optical network unit, an echo of a capability of said optical line terminal, a session key, a nonce decrypted by a public key of said optical line terminal, and a nonce created for signature of said optical network unit.

25

18. The session key distribution method as set forth in claim 17, wherein said physical ID capability, said capability of said optical network unit, said echo of said capability of said optical line terminal, said nonce decrypted by said public
5 key of said optical line terminal and said nonce created for the signature of said optical network unit are encrypted using said session key.

19. The session key distribution method as set forth in
10 claim 17, wherein said session key is encrypted using said public key of said optical line terminal.

20. The session key distribution method as set forth in claim 14, wherein said registration message further includes a
15 physical ID list, an echo of a capability of said optical network unit, and a signature of said optical network unit.

21. The session key distribution method as set forth in claim 14, wherein said general gate message further includes a
20 time slot field for upstream transmission of said optical network unit.

22. The session key distribution method as set forth in claim 21, wherein said general gate message is encrypted using
25 a session key.

23. The session key distribution method as set forth in claim 14, wherein said registration acknowledgement message includes a session key encrypted by a public key of said optical line terminal, and an echo of a registered physical ID.

5

24. The session key distribution method as set forth in claim 23, wherein said registration acknowledgement message is encrypted using said session key.

10 25. A method for session key update between an optical line terminal and an optical network unit in a key management method for provision of a security service in an Ethernet-based passive optical network, comprising the steps of:

15 a), by said optical line terminal, sending key update information to said optical network unit at a predetermined key update period; and

b), by said optical network unit, receiving said key update information and sending a new session key to said optical line terminal.

20

26. The session key update method as set forth in claim 25, further comprising the steps of:

25 c), by said optical line terminal, storing said session key from said optical network unit in a storage unit allocated thereto; and

d), by said optical network unit, storing said session key in a session key storage unit therein.

27. The session key update method as set forth in claim
5 25, wherein said key update information is sent to said optical network unit through a general gate message.

28. The session key update method as set forth in claim
25, wherein said new session key is sent to said optical line
10 terminal through a report message.

29. A method for key recovery between an optical line terminal and an optical network unit in a key management method for provision of a security service in an Ethernet-
15 based passive optical network, comprising the steps of:

a) determining whether a pair of private and public keys are in error;

b), if said pair of private and public keys are in error, by said optical line terminal, creating a pair of new
20 private and public keys and multicasting the new public key while including it in a desired message; and

c), by said optical network unit, receiving said new public key, comparing it with a public key pre-stored in a public key storage unit therein, discarding said new public
25 key if it is the same as the pre-stored public key and storing

said new public key in said public key storage unit if it is different from the pre-stored public key.

30. The key recovery method as set forth in claim 29,
5 wherein said step a) includes the step of, by said optical line terminal or optical network unit, detecting a private/public key error by decrypting a received message using a session key and verifying a frame check sequence for the decrypted message.

10 31. The key recovery method as set forth in claim 29, wherein said new public key created by said optical line terminal is sent to said optical network unit while being included in a discovery gate message.

15 32. A method for key recovery between an optical line terminal and an optical network unit in a key management method for provision of a security service in an Ethernet-based passive optical network, comprising the steps of:

20 a) determining whether there is a session key error between said optical line terminal and said optical network unit; and

b), if there is a session key error between said optical line terminal and said optical network unit, by said optical
25 network unit, sending a new session key to said optical line

terminal using a time slot sent while being included in a discovery gate message.

33. The key recovery method as set forth in claim 32,
5 wherein said step a) includes the step of determining that there is a session key error between said optical line terminal and said optical network unit, if there is not continuously present any upstream transmission from said optical network unit pre-allocated a time slot from said optical line
10 terminal.

34. The key recovery method as set forth in claim 32, wherein said step a) includes the step of determining that there is a session key error between said optical line terminal
15 and said optical network unit, if said optical network unit periodically receives said discovery gate message from said optical line terminal, but does not continuously receive a general gate message from said optical line terminal.

20 35. The key recovery method as set forth in claim 32, wherein said new session key created by said optical network unit is sent to said optical line terminal while being included in a report message.

25